

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-324936

(43)Date of publication of application : 10.12.1993

(51)Int.Cl.

G06K 17/00  
 B42D 15/10  
 B42D 15/10  
 G07F 7/08  
 G09C 1/00  
 // G11B 13/00

(21)Application number : 04-148426

(71)Applicant : DAINIPPON PRINTING CO LTD

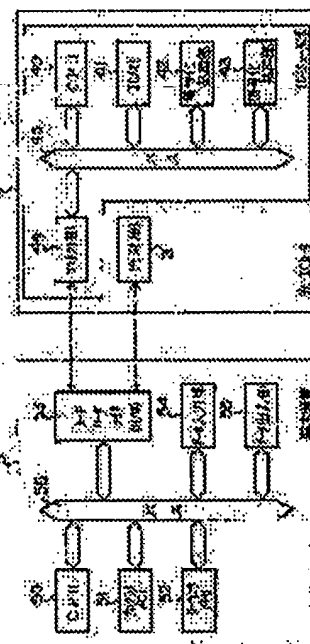
(22)Date of filing : 15.05.1992

(72)Inventor : TODA AKIRA

## (54) RECORDING AND REPRODUCING SYSTEM FOR OPTICAL IC CARD

## (57)Abstract:

**PURPOSE:** To provide the recording and reproducing system which can limit the users of data recorded in a card or registered persons to record data in the card.  
**CONSTITUTION:** This system is provided with a cipher processing part 42 to cipher data to be recorded in a prescribed cipher sequence with an arbitrary cipher key, recording means to record the ciphered data in an optical memory part 3 of a card 1, reading means to read the data recorded in the optical memory part 3, and decipher processing part 43 to decipher the data read by the reading means according to a prescribed decipher sequence with an arbitrary decipher key, and the cipher key and decipher key are composed of keys in a pair of public cipher systems of which contents are different from each other.



## LEGAL STATUS

[Date of request for examination] 30.04.1999

[Date of sending the examiner's decision of rejection] 26.12.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-324936

(43)公開日 平成5年(1993)12月10日

(51)IntCl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 17/00	E	7459-5L		
B 4 2 D 15/10	5 1 1	9111-2C		
	5 2 1	9111-2C		
G 0 7 F 7/08		7130-3E	G 0 7 F 7/08	A

審査請求 未請求 請求項の数3(全11頁) 最終頁に続く

(21)出願番号 特願平4-148426

(22)出願日 平成4年(1992)5月15日

(71)出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72)発明者 戸田 明

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

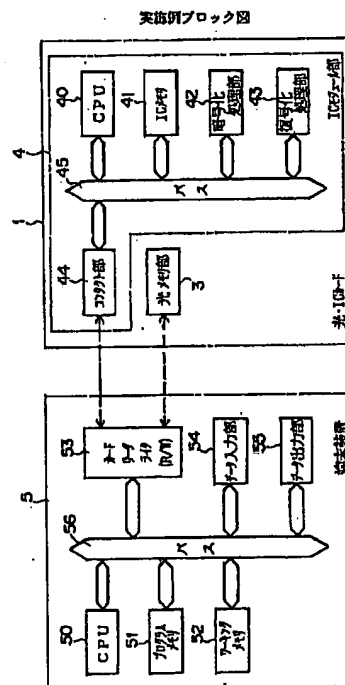
(74)代理人 弁理士 録田 久男

(54)【発明の名称】 光・ICカードの記録再生システム

(57)【要約】

【目的】 光・ICカードの記録再生システムに関し、カードに記録してあるデータの利用者、あるいはカードにデータを記録できる登録者を限定することのできる記録再生システムを提供することを目的とする。

【構成】 記録するデータを任意の暗号化鍵によって所定の暗号化手順で暗号化する暗号化処理部と、暗号化したデータをカード内の光メモリ部に記録する記録手段と、光メモリ部に記録したデータを読み取る読取手段と、読取手段で読み取ったデータを任意の復号化鍵によって所定の復号化手順で復号する復号化処理部とを設け、暗号化鍵および復号化鍵は互いに内容の異なる一対の公開暗号系の鍵で構成する。



## 【特許請求の範囲】

【請求項1】 記録するデータを任意の暗号化鍵によって所定の暗号化手順で暗号化する暗号化処理部と、前記暗号化したデータをカード内の光メモリ部に記録する記録手段と、

前記光メモリ部に記録したデータを読み取る読取手段と、

前記読取手段で読み取ったデータを任意の復号化鍵によって所定の復号化手順で復号する復号化処理部とを備え、

前記暗号化鍵および前記復号化鍵は互いに内容の異なる一対の公開暗号系の鍵で構成したことを特徴とする光・ICカードの記録再生システム。

【請求項2】 請求項1において、前記暗号化鍵は前記カード内に予め記録しておき、前記復号化鍵は当該カード使用者が端末装置から入力することを特徴とする光・ICカードの記録再生システム。

【請求項3】 請求項1において、前記暗号化鍵は当該カード使用者が端末装置から入力し、前記復号化鍵は前記カード内に予め記録しておくことを特徴とする光・ICカードの記録再生システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、光学的に情報の記録・再生が可能な光メモリ部と中央処理装置を含む集積回路部とを一体化してカード状に構成した光・ICカードの記録再生システムに関する。

## 【0002】

【従来の技術】 従来からカードの表面の一部に磁気的な記録部を設けたキャッシュカード、クレジットカードおよびテレホンカードなどカード化された記録媒体が幅広く使用されている。カードは携帯性の利便さにおいて他の記録媒体に対し優位性を有しており、この特徴を活かした用途開発が活発になされている。最近では、カードの利用分野を広げるために、カードにより大きな記録容量およびより高度な機能が求められ、この要求を満たすためのカードとして光カードおよびICカードなどが開発されている。

【0003】 光カードは光ディスク技術を応用して情報をレーザ光で書き込み、この書き込んだ情報を光センサを有する読取装置にかけて読み取るもので、約5千万文字の情報を記録することが出来る。ICカードは半導体集積回路技術を用いて構成した中央処理装置（CPU）を含む集積回路部（以下、ICモジュール部、という）を内部に実装しているカードで、高度な判断、高速演算、データ処理等のインテリジェント機能を備え、記録容量は光カードほど膨大ではないが、約8千文字の情報を記録することが出来る。

【0004】 光カードは情報記録容量が飛躍的に大きいばかりでなく、製造工程が簡単で短時間で大量生産がで

きるため、低コスト化が図れるという利点を有する反面、情報記録面を顕微鏡などの簡易な光学系を用いて単に拡大して見ることにより情報内容を読み取ることができ、情報の秘匿性は低いという欠点がある。これに対し、ICカードは記録情報をICモジュール部のメモリに記録し、CPUの働きによって入出力情報を全て電子的に処理することができるため、高度の情報秘匿性を得ることができる反面、製造コストが高く、1枚のカードに記録できる情報量も光カードに比べると格段に低いという欠点がある。

【0005】 そこで、最近では光カードの大容量記録性とICカードの情報秘匿性およびインテリジェント性を考慮して1枚のカードに光メモリ部とICモジュール部とを一体的に設けた光・ICカードが提案されている。そして、光・ICカードのこの特性を利用して病院のカルテなどの個人医療記録管理、貯金通帳などの金銭管理、企業内シークレットを含む機器保守管理、文書管理など広い範囲に利用することが検討されている。

## 【0006】

【発明が解決しようとする課題】 ところで、光・ICカードは前述したように広い範囲での利用が可能であるため様々な使用態様が考えられる。例えば、カードへのデータの記録は使用者を特定せずにある程度自由に行うことができ、カードに記録してあるデータの再生は特定の者しか行えないようにするシステムが考えられる。また、これとは逆にカードへのデータの記録は特定の者しか行えず、カードに記録してあるデータの再生は使用者を特定せずにある程度自由に行えるようにするシステムも考えられる。

【0007】 前者の例としては、カードを医療用カルテとして使用する場合に、各医療部門で検査結果や診療結果をカードに記録し、記録したデータの再生は限られた特定の者、例えば担当医にしか行えないようにするシステムがそれである。また、後者の例としては、カードを医療用カルテとして使用する場合に、処方箋に関するデータは担当医のみが記録できるようにし、データの再生は薬剤師であれば特定の者でなくても再生できるようにするシステムがそれである。

【0008】 ところが、従来のカードシステムでは、カードへのデータの記録またはカードからのデータの再生は使用者が正しいパスワードを入力しさえすれば可能であるため、第三者にパスワードを知られてしまうとデータの記録または再生が容易になされてしまうという不都合がある。しかも、カードに記録されているパスワードは多少の専門知識を有する者にとっては解読可能であり、現在の磁気カードでも実際に解読される被害が生じている。ICカードはICメモリ内にパスワードを記録しておくため、磁気カードや光カードに比べると秘匿性は保たれるが、それでも数桁のパスワードの解読は不可能ではない。

【0009】また、光メモリ部は大容量のデータを記録することが出来るが、記録したデータは前述したように簡易な光学系を用いて読み取ることが出来るため、情報の秘匿性が低いという不都合がある。

【0010】本発明は、カードに記録してあるデータの利用者、あるいはカードにデータを記録できる登録者を限定することのできる記録再生システムを提供することを目的とする。

【0011】

【課題を解決するための手段】本発明による光・ICカードの記録再生システムは、記録するデータを任意の暗号化鍵によって所定の暗号化手順で暗号化する暗号化処理部と、暗号化したデータをカード内の光メモリ部に記録する記録手段と、光メモリ部に記録したデータを読み取る読取手段と、読取手段で読み取ったデータを任意の復号化鍵によって所定の復号化手順で復号する復号化処理部とを設け、暗号化鍵および復号化鍵は互いに内容の異なる一対の公開暗号系の鍵で構成する。この場合、暗号化鍵はカード内に予め記録しておき、復号化鍵は当該カード使用者が端末装置から入力するように構成する。また、この場合、暗号化鍵は当該カード使用者が端末装置から入力し、復号化鍵はカード内に予め記録するように構成する。

【0012】

【作用】本発明は暗号化鍵と復号化鍵とが互いに異なる公開鍵暗号系を使用し、一方の鍵を秘密鍵、他方の鍵を公開鍵とすることによってカードに記録してあるデータの利用者、あるいはカードにデータを記録できる登録者を限定することができるようになっている。

【0013】カードに記録してあるデータの利用者を限定するときは、暗号化鍵は公開鍵として予めカード内に記録しておき、復号化鍵は秘密鍵として使用者が端末装置から入力するようにする。カードにデータを記録するときは、使用者が端末装置から記録データを入力し、カード内に記録してある暗号化鍵によって入力したデータを暗号化処理部で暗号化し、暗号化したデータを光学的な記録手段によって光メモリ部に記録する。

【0014】カード内に記録してあるデータを再生するときは、光学的な読取手段によって光メモリ部からデータを読み取り、使用者が端末装置から復号化鍵を復号化処理部に入力することによって行う。復号化処理部では、入力された復号化鍵を用いて所定の復号化手順でデータを復号し再生する。

【0015】したがって、カードへのデータの記録は暗号化鍵を知らなくても可能であり、使用者を限定せずにある程度自由に行うことが出来る。これに対し、カードに記録してあるデータの再生は、復号化鍵を知っている者しか行うことができないため、データの利用は特定の者しか行うことが出来ない。

【0016】カードにデータを記録できる登録者を限定

するときは、暗号化鍵は秘密鍵として使用者が端末装置から入力するようにし、復号化鍵は公開鍵として予めカード内に記録しておく。カードにデータを記録するときは、使用者が端末装置から暗号化鍵を暗号化処理部に入力することによって行う。暗号化処理部では、この暗号化鍵を用いて所定の暗号化手順で記録するデータを暗号化し、暗号化したデータは光学的な記録手段を用いてカード内の光メモリ部に記録する。

【0017】カード内に記録してあるデータを再生するときは、光学的な読取手段によって光メモリ部からデータを読み取り、予めカード内に記録してある復号化鍵を用いて復号化処理部で所定の復号化手順でデータを復号し再生する。

【0018】したがって、カードへのデータの記録は暗号化鍵を知っている特定の者しか行うことが出来ず、これに対してカードに記録してあるデータの再生は、使用者が復号化鍵を知らなくても行うことができ、使用者を限定せずにある程度自由に行うことが出来る。

【0019】

【実施例】図1は、本発明で使用する光・ICカード1の平面図で、プラスチック製のカード基材2上に光メモリ部3および集積回路部（ICモジュール部）4を形成した構成となっている。

【0020】光メモリ部3はレーザ光の照射によって情報が書き込まれ、弱いレーザ光の反射光によって記録されている情報が読み出される大容量の情報記録部である。この光メモリ部3は、図2の縦断面図に示すように、非銀塩パターン層30に低反射部31（反射率5%）が形成され、その下面にアルミニウム反射層32（反射率80%）を蒸着して情報記録層としている。情報記録層は透明な保護層33とカード基材層（基板）34とで挟持されており、保護層33の表面には傷が付くのを防止するために表面硬化層35が設けられている。

【0021】光メモリ部3には、カード1の長手方向に複数のバンドBがカード1の短手方向に平行に並んで形成されており、情報領域が構成されるようにフォーマット化されている。また、各バンドBには数バイトのデータを含むトラックが多数横に並んで形成されており、各トラックを構成する情報ビットはビットセルと呼ばれる単位領域毎に低反射部31の有無または低反射部31の位置で2値信号として記録されている。

【0022】ICモジュール部4は半導体集積回路技術によって構成したCPUやメモリなどのICチップをプリント基板上に組み込み、カード基材2内に埋め込むなどして装着したもので、カード1の表面にはISO（国際標準化機構）で定めた規格位置に後述するカード用端末装置との接続を図る6個の端子C1～C6が露出している。この端子C1～C6は端末装置からの電源電圧の供給、端末装置との間のデータ伝送などに使用される。

【0023】図3は、本発明による光・ICカードの記

録再生システムの一例を示すブロック図である。同図において、光・ICカード1は前述したように光メモリ部3およびICモジュール部4を有し、ICモジュール部4内にはCPU40、ICメモリ41、平文を暗号処理する暗号化処理部42、暗号文を復号処理する復号化処理部43、端子C1～C6を含むコンタクト部44がそれぞれバス45を介して接続されている。

【0024】また、カード用端末装置5は、CPU50、プログラムメモリ51、ワーキングメモリ52などの通常のコンピュータシステムのほかに、カード1が挿入されるカードリーダーライタ部（以下、R/W部、という）53、パスワードや記録データなどを入力するキーボード装置やディスクドライブ装置などのデータ入力部54、使用者に対する操作手順の指示や再生データの出力などを行うディスプレイ装置やプリンタ装置などのデータ出力部55がそれぞれバス56を介して接続されている。

【0025】R/W部53は手動または自動によって挿入・排出されるカード1のコンタクト部44と結合してICモジュール部4へ電源を供給したり、クロック信号やリセット信号等の制御信号を供給したり、ICモジュール部4および端末装置5間のデータ送受を制御したりすると共に、内蔵されている光ヘッド装置によって光メモリ部3に対するデータの記録・再生を行うように構成されている。

【0026】次に、端末装置5にカード1を挿入してデータの記録および再生を行う場合の処理手順について、図4～図7に示すシーケンス図を参照して説明する。なお、いずれの処理の場合もパスワードの照合は既に完了しているものとする。まず、本発明で使用する暗号系について説明する。本発明で使用する暗号系は暗号化鍵と復号化鍵とが異なり、しかも一方の鍵は公開しても差し支えない公開鍵暗号系で、代表的なものに3人の発案者の頭文字を取ったRSA (Rivest, Shamir, Adleman)暗号がある。暗号内容の詳細については公知文献（例えば、「暗号と情報セキュリティ」、辻井・笠原編著）に譲るが、この暗号は大きな数の素因数分解の困難さに安全性の根拠をおき、べき乗剰余の計算により暗号化/復号化処理を行うものである。

【0027】暗号化手順Eは「 $C = E(M) = M^e \bmod n$ 」で表され、復号化手順Dは「 $M = D(C) = C^d \bmod n$ 」で表される。Mは平文、Cは暗号文である。暗号化鍵はeとn、復号化鍵はdとnで、暗号化鍵eとnは公開し、復号化鍵dは秘密とする。鍵e, d, nの決定は次の手順で行う。

② 2つの大きな素数p, qを任意に選び、 $n = pq$ とする。

③  $(p-1)$ と $(q-1)$ の最小公倍数Lを計算し、Lと互いに素でLより小さな任意の整数eを求める。

④  $ed = 1 \pmod{L}$ を満たすdを求める。

こうして選んだ値e, d, nは、全ての平文Mに対し、「 $Med \bmod n = M$ 」が成立する。

【0028】解読者が暗号文Cを解読するには復号化鍵dを知らなければならないが、そのためには秘密の素数p, qを知り、 $(p-1)$ および $(q-1)$ の最小公倍数Lと公開鍵eとから「 $d = e^{-1} \pmod{L}$ 」を演算し、秘密鍵dを求める必要がある。公開鍵nは素数pとqの積であるから公開鍵nが容易に素因数分解できる程度の整数では暗号にならない。通常はpとqを各100桁（十進数）程度とし、公開鍵nは200桁程度としている。こうすれば、1000 MIPSの電子計算機を用いても素因数分解に数百万年かかる勘定になり、実質的に解読は不可能である。

【0029】次に、図4および図5に示すシーケンス図を参照し、本発明による第1の動作実施例について説明する。本実施例はカードへのデータの記録はある程度自由に行うことができ、しかしながらカードからのデータの再生は特定の者しか行うことができないようにした例である。このため、暗号化鍵e, nは公開鍵としてカード1内に予め記憶しておき、復号化鍵dは秘密鍵として再生時にカード使用者が端末装置5から入力するようにする。

【0030】まず、記録処理の場合は、図4のシーケンス図に示すように、使用者が端末装置5のデータ入力部54から記録データMeを入力することによって開始する。記録データMeの入力は、使用者によるキーボード装置からの直接入力、予め磁気ディスク等に記録したデータのドライブ装置からの転送などがある。

【0031】入力された記録データMeはバス56を通り、R/W部53およびカード1のコンタクト部44を経て暗号処理部42へ転送される（ステップS1）。暗号化処理部42へはICメモリ部41に公開鍵として予め記憶してある暗号化鍵e, nが供給されているので（ステップS2）、暗号処理部42では暗号化鍵e, nを用いて記録データMeを所定の暗号化手順Eで暗号化し、暗号データC（ $= Me^e \bmod n$ ）を生成する。

【0032】生成された暗号データCはバス45を通り、コンタクト部44から端末装置5のR/W部53に転送され（ステップS3）、R/W部53内の光ヘッド装置によってカード1内の光メモリ部3に記録される（ステップS4）。

【0033】次に、カード1の光メモリ部3に記録されているデータを再生するには、図5のシーケンス図に示すように、使用者が端末装置5のデータ入力部54から復号化鍵dを入力することによって開始する。入力された復号化鍵dはバス56を通り、R/W部53およびカード1のコンタクト部44を経ていったんICメモリ41に記憶される（ステップS5）。

【0034】次いで、R/W部53内の光ヘッド装置で光メモリ部3に記録されている暗号データCの読み取り

を行い(ステップS6)、読み取った暗号データCはコンタクト部44を介してICモジュール部4内の復号化処理部43に転送する(ステップS7)。復号化処理部43へは、ICメモリ41から復号化鍵d, nが供給されているので(ステップS8)、復号化処理部43ではこの復号化鍵d, nを用いて所定の復号化手順Dで暗号データCを復号処理し、再生データMd ( $=C^d \bmod n$ )として出力する。

【0035】復号された再生データMdはコンタクト部44からR/W部53を経てデータ出力部55へ転送され(ステップS9)、ディスプレイ装置やプリンタ装置などを介して外部に出力される。

【0036】次に、図6および図7に示すシーケンス図を参照し、本発明による第2の動作実施例について説明する。本実施例はカードへのデータの記録は特定の者しか行えず、しかしながらカードからのデータ再生は使用者を限定せずにある程度自由に行うことができるようにした例である。このため、暗号化鍵eは秘密鍵としてデータ記録時にカード使用者が端末装置5から入力するようにし、復号化鍵d, nは公開鍵としてカード1内に予め記憶しておくようにする。

【0037】まず、記録処理の場合は、図6のシーケンス図に示すように、使用者が端末装置5のデータ入力部54から暗号化鍵eを入力する。入力された暗号化鍵eはバス56を通り、R/W部53およびカード1のコンタクト部44を経ていったんICメモリ41に記憶される(ステップS10)。次いで、端末装置5のデータ入力部54から記録データMeを入力する。記録データMeの入力は、使用者によるキーボード装置からの直接入力、磁気ディスクに予め記録したデータのドライブ装置からの転送などがある。

【0038】入力された記録データMeはバス56を通り、R/W部53およびカード1のコンタクト部44を経て暗号処理部42へ転送される(ステップS11)。暗号化処理部42へはICメモリ部41から暗号化鍵e, nが供給されるので(ステップS12)、暗号処理部42では暗号化鍵e, nを用いて記録データMeを所定の暗号化手順Eで暗号化し、暗号データC ( $=Me^e \bmod n$ )を生成する。

【0039】生成された暗号データCはバス45を通り、コンタクト部44から端末装置5のR/W部53に転送され(ステップS13)、R/W部53内の光ヘッド装置によってカード1内の光メモリ部3に記録される(ステップS14)。

【0040】次に、こうしてカード1の光メモリ部3に記録したデータを再生するには、図7のシーケンス図に示すように、光メモリ部3に記録されている暗号データCをR/W部53内の光ヘッド装置で読み取る(ステップS15)。読み取った暗号データCはコンタクト部44を介してICモジュール部4内の復号化処理部43に

転送する(ステップS16)。

【0041】復号化処理部43へはICメモリ41から復号化鍵d, nが供給されているので(ステップS17)、復号化処理部43では復号化鍵d, nを用いて所定の復号化手順Dで暗号データCを復号処理し、再生データMd ( $=C^d \bmod n$ )を出力する。

【0042】再生データMdはコンタクト部44からR/W部53を経てデータ出力部55へ転送され(ステップS18)、ディスプレイ装置やプリンタ装置などの出力装置を介して外部に出力される。

【0043】なお、前述の実施例では、カード内に暗号化処理部および復号化処理部を設置するようにしたが、これらのロジック部は汎用化されているので、カード内に設置しても、端末装置内に設置しても、あるいは両方に設置してもよい。また、使用する暗号系としては、前述したRSA暗号系に限らず、暗号アルゴリズムが公開されている他の公開鍵暗号系であってもよい。

【0044】

【発明の効果】本発明によれば、暗号化鍵および復号化鍵のうち、一方の鍵を秘密鍵、他方の鍵を公開鍵とすることによってカードに記録してあるデータの利用者、あるいはカードにデータを記録できる登録者を限定することができる。したがって、暗号化鍵を公開鍵、復号化鍵を秘密鍵とすれば、カードへのデータ記録は使用者を限定せずにある程度自由に行うことができ、カードからのデータ再生は復号化鍵を知っている特定の者しか行うことができない。また、暗号化鍵を秘密鍵、復号化鍵を公開鍵とすれば、カードへのデータ記録は暗号化鍵を知っている特定の者しか行うことができず、カードからのデータ再生は使用者を限定せずにある程度自由に行うことができる。

【図面の簡単な説明】

【図1】本発明で使用する光・ICカードの平面図である。

【図2】図1に示す光・ICカードの光メモリ部の部分断面図である。

【図3】本発明の一実施例を示すブロック図である。

【図4】本発明の第1の動作実施例のうち記録処理を示すシーケンス図である。

【図5】本発明の第1の動作実施例のうち再生処理を示すシーケンス図である。

【図6】本発明の第2の動作実施例のうち記録処理を示すシーケンス図である。

【図7】本発明の第2の動作実施例のうち再生処理を示すシーケンス図である。

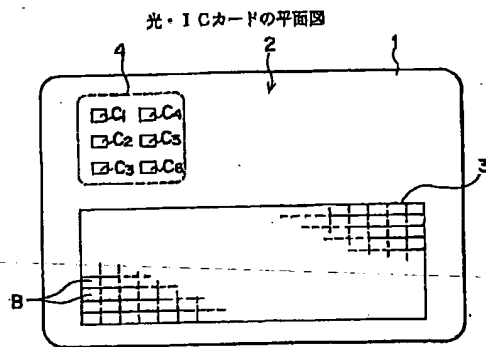
【符号の簡単な説明】

- 1 光・ICカード
- 2 カード基材
- 3 光メモリ部
- 4 ICモジュール部

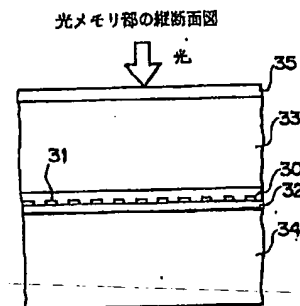
- 5 カード用端末装置
- 40 CPU
- 41 ICメモリ
- 42 暗号化処理部
- 43 復号化処理部
- 44 コンタクト部
- 45 バス

- 50 CPU
- 51 プログラムメモリ
- 52 ワーキングメモリ
- 53 カードリーダーライタ部 (R/W部)
- 54 データ入力部
- 55 データ出力部
- 56 バス

【図1】



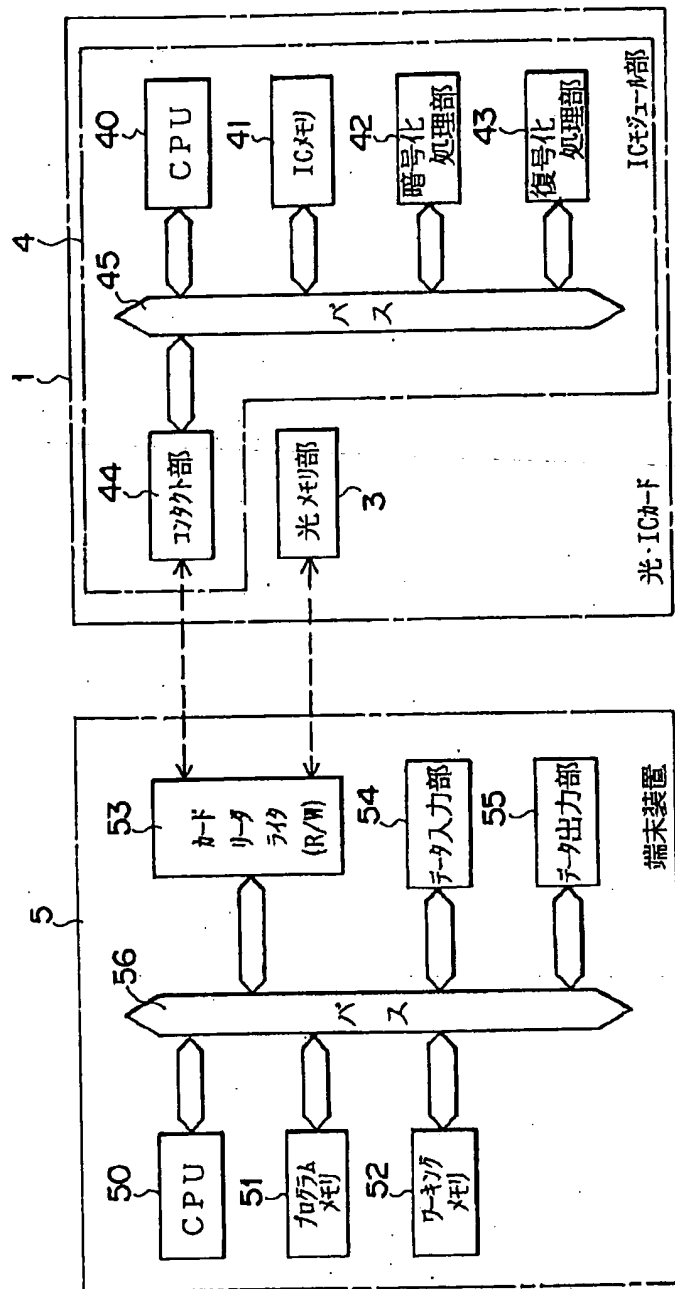
【図2】





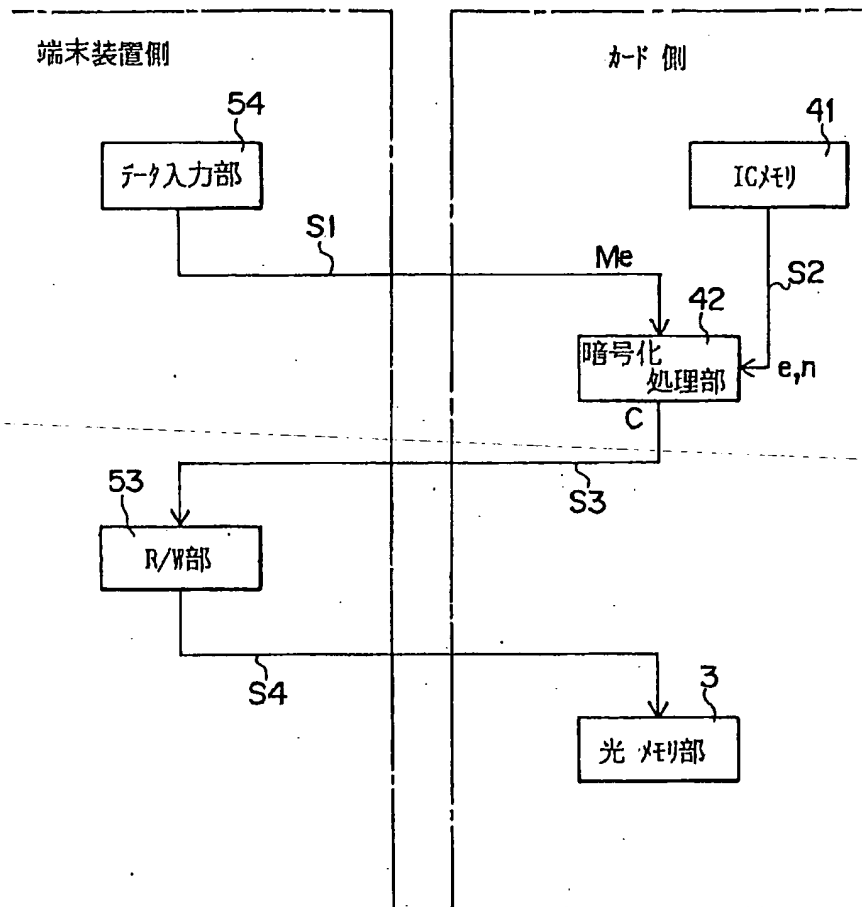
【図3】

実施例ブロック図



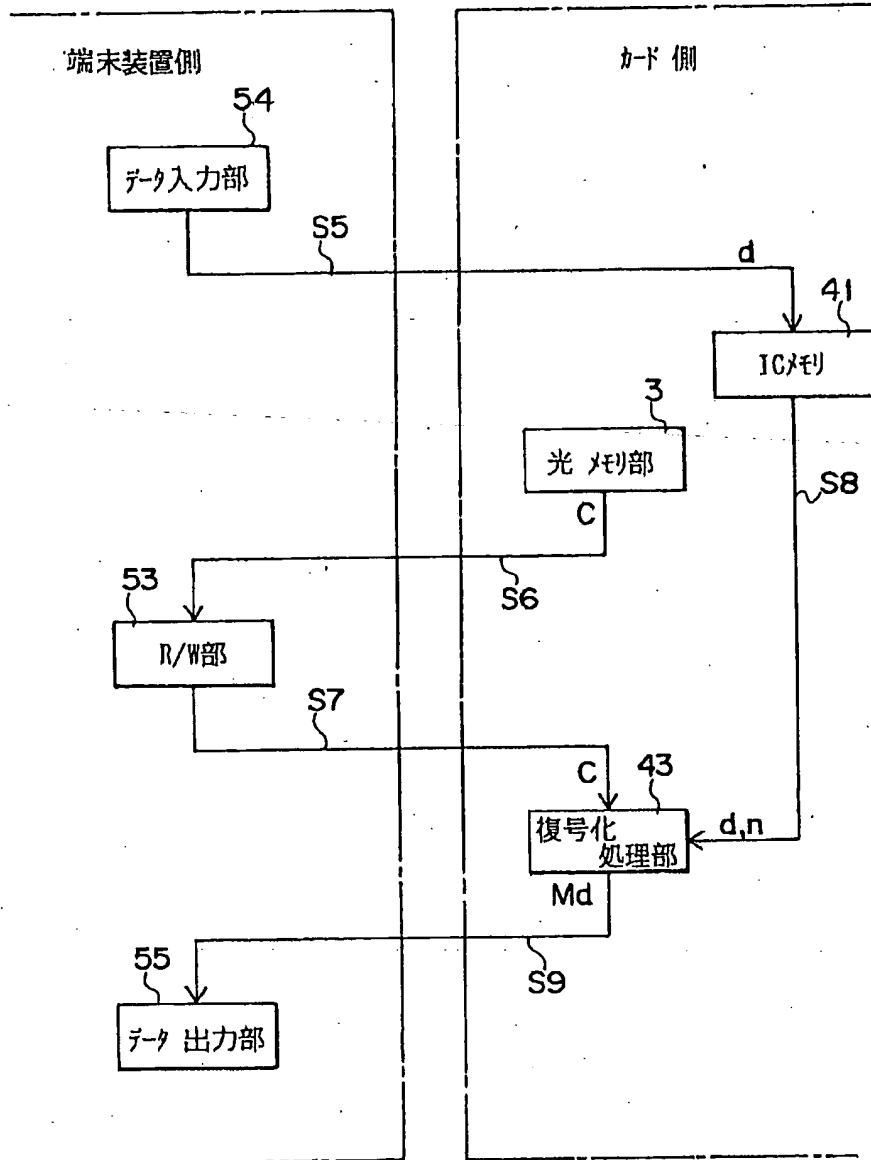
【図4】

## 第1の実施例の記録処理



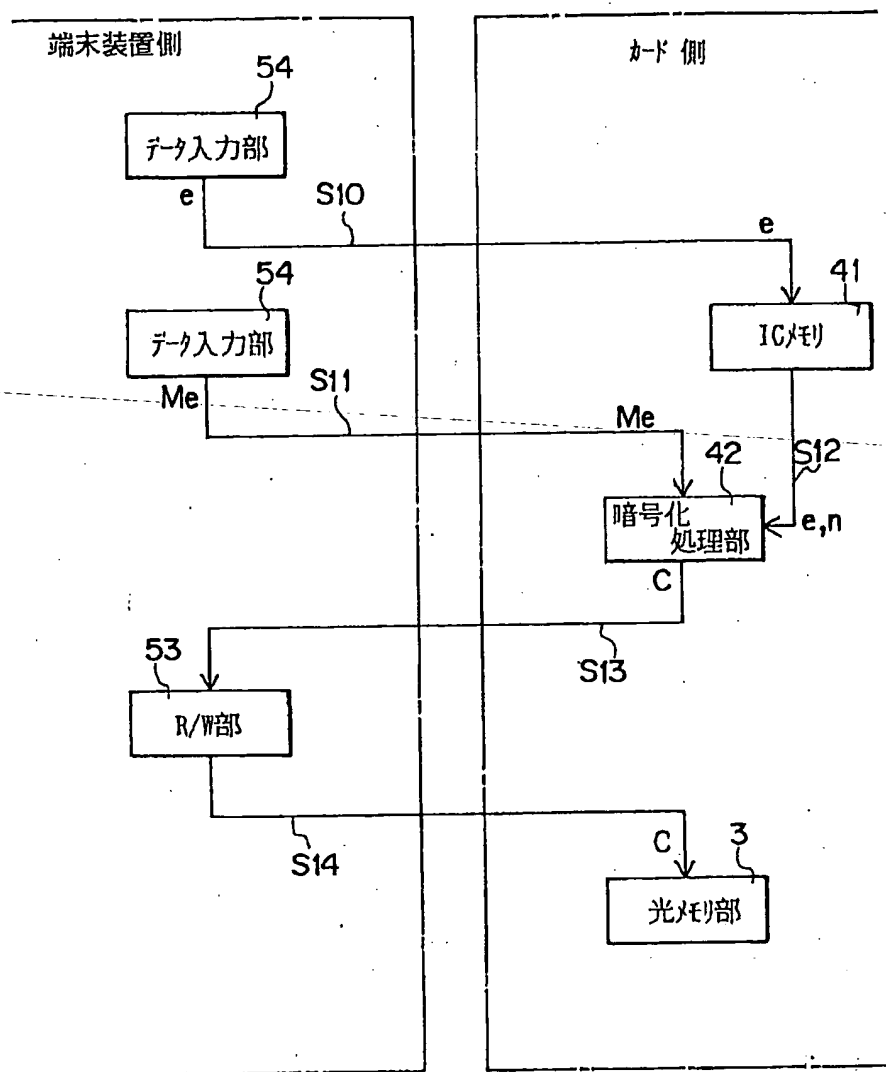
【図5】

## 第1の実施例の再生処理



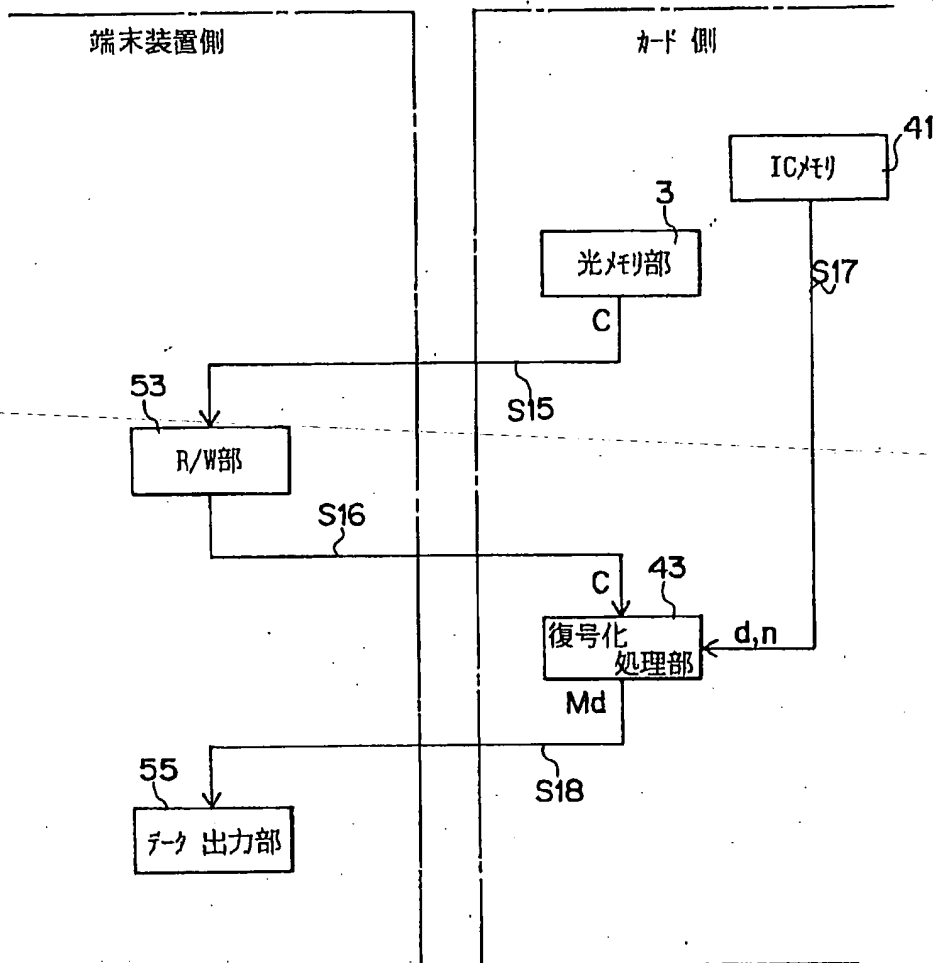
【図6】

## 第2の実施例の記録処理



【図7】

## 第2の実施例の再生処理



フロントページの続き

(51)Int.Cl.<sup>5</sup>

G 0 9 C 1/00

// G 1 1 B 13/00

識別記号

庁内整理番号

9194-5L

9075-5D

F I

技術表示箇所